## AMENDMENTS TO THE CLAIMS

This listing of claims replaces all prior versions and listings of claims in the application.

Listing of Claims

1 – 31. (Canceled)

32. (New) A method of issuing an electronic coin, comprising:

receiving a plurality of values, each value being a function of a pre-image of an electronic coin;

for each received value, populating a leaf of a hash tree with a function of the received value;

publicly distributing roots of the hash tree, wherein the roots of the hash tree may be used to verify the validity of the electronic coin to be issued and to audit a supply of electronic coins.

33. (New) The method of claim 32, wherein the pre-image of the electronic coin is a function of a serial number and a random number.

34. (New) The method of claim 32, further comprising verifying that the electronic coin is well formed.

35. (New) The method of claim 32, further comprising issuing the electronic coin.

36. (New) The method of claim 35, further comprising crediting the account of a merchant in the amount of the issued electronic coin.

37. (New) The method of claim 35, further comprising:

removing the leaf corresponding to the electronic coin;

updating the hash tree; and

distributing the roots of the updated hash tree.

38. (New) The method of claim 37, wherein distributing the roots of the hash tree comprises providing controlled access.

39. (New) The method of claim 37, wherein distributing the roots of the hash tree comprises making the roots accessible to the general public.

40. (New) A method of auditing a supply of electronic coins in an electronic monetary system, comprising:

accessing a hash tree that is a function of a plurality of leaves, each leaf being a function of a pre-image of an electronic coin that has not been withdrawn;

accessing withdrawal records corresponding to coins that have been withdrawn and accessing a public list of roots of the hash tree;

verifying the validity of the supply of electronic coins in the electronic monetary system.

41. (New) The method of claim 40, wherein each of the withdrawal records corresponds uniquely to one of the withdrawn coins.

42. (New) The method of claim 41, wherein the validity of the supply of electronic coins is verified without knowledge of which withdrawal record corresponds to which withdrawn coin.

43. (New) A method of redeeming an electronic coin, comprising:

receiving a public set of roots of a hash tree;

receiving a pre-image value of the electronic coin from a customer;

sending the public set of roots of the hash tree to the customer;

receiving from the customer a zero knowledge proof that the roots of the hash tree are a function of the electronic coin.

44. (New) The method of claim 43, wherein the customer may remain anonymous by not revealing the serial number of the electronic coin.

45. (New) The method of claim 43, further comprising periodically receiving an updated public set of roots of the hash tree.

46. (New) The method of claim 43, further comprising transferring goods or services to the customer.

47. (New) The method of claim 46, further comprising sending a payment transcript to an issuer of the electronic coin.